



# Department of Homeland Security Daily Open Source Infrastructure Report for 19 April 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](#)

<http://www.dhs.gov/>

## Daily Highlights

- The Associated Press reports Texas cities suffered in record high temperatures Monday, April 17, and power suppliers urged Texans to cut down on their electricity use in the hope of avoiding continuing rolling blackouts. (See item [1](#))
- KOMO TV reports that for 25 minutes in the early hours of April 11, the control tower at Seattle–Tacoma International Airport did not respond to airplane traffic, prompting an investigation by the Federal Aviation Administration. (See item [17](#))
- The Associated Press reports Nebraska, which is part of a nine–state mumps epidemic, is now reporting 110 cases of the disease in 22 counties; the mumps epidemic is the nation's first in 20 years. (See item [27](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – <http://www.esisac.com>]

1. *April 18, Associated Press* — **Record heat leads to power outages in Texas.** Texas cities baked in record high temperatures Monday, April 17, and power suppliers urged Texans to cut down on their electricity use in the hope of avoiding more rolling blackouts. Power companies throughout the state imposed the blackouts Monday because of an electricity shortage during

unseasonably hot weather. Thousands of people were caught without electricity for short periods of time as highs reached into the low 100s. As much as 15 percent of the state's power supply was already off line for seasonal maintenance to brace for the summer's energy usage peaks, but four power generating plants also shut down unexpectedly, Paul Wattles, spokesperson for Electric Reliability Council of Texas (ERCOT), which runs the state's electricity grid, said. Officials were pushing to get power flowing again from the generators that had been idled. ERCOT said operations were back to normal by Monday evening. The typical usage for Texas in April is about 40,000 megawatts a day, but the state pushed 52,000 megawatts on Monday, said Wattles. The rollouts were limited to the ERCOT grid, which provides electricity to about 80 percent of the state. The rolling blackouts lasted for a little more than two hours.

Source: <http://www.cnn.com/2006/WEATHER/04/18/texas.blackouts.ap/index.html>

2. *April 18, Los Angeles Times* — **Utilities will fund studies for California power plan.** Seven utilities agreed Monday, April 17, to bankroll economic and environmental studies for a massive transmission line that would bring cheap electricity to California from generating plants as far away as northern Wyoming. The utilities, including Southern California Edison Co., Pacific Gas and Electric Co. and San Diego Gas and Electric Co., said they formed a partnership to study future demand in California and potential routes for the 1,300-mile transmission line. The so-called "Frontier Line" could cost \$6 billion and take six years to build. It would be one of the largest in the country, carrying upward of 14,000 megawatts of electricity — enough to serve more than 10 million homes and businesses in California and other Western states. The power would be produced from a variety of sources — including wind and coal.

Source: <http://www.stltoday.com/stltoday/news/stories.nsf/metroeast/story/23642FC8E8F5DC2E862571540013F1D0?OpenDocument>

3. *April 18, Associated Press* — **Oil prices hit new record of \$70.88.** Oil prices reached a new high of \$70.88 a barrel Tuesday, April 18, as persistent concerns about Iran's nuclear program and supply disruptions in Nigeria overshadowed a new report from the Organization of the Petroleum Exporting Countries (OPEC) forecasting weakening global demand. In its latest monthly report, OPEC on Tuesday revised its demand-growth forecast for 2006 to 1.42 million barrels a day, down from 1.46 million barrels per day in the previous report. The cartel estimates that global crude-oil demand will be slightly above 84.5 million barrels per day — about half a million barrels per day lower than the current Wall Street consensus. Still, analysts said oil prices were likely to climb further as long as geopolitical risks in Iran and Nigeria posed threats to supply. Crude oil production is only barely keeping up with rising global demand, leaving a slim margin for error if there is a prolonged supply interruption, experts say. Also underpinning high oil prices is booming demand in emerging economies such as China and India.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/04/18/AR2006041800236.html>

4. *April 17, Reuters* — **BP discloses another Alaska pipeline leak.** BP's Alaska unit said on Monday, April 17, corrosion caused another pipeline leak a month after a crude oil pipeline leak created the biggest oil spill on record at the state's North Slope. BP discovered the new leak on Thursday, April 6, involving a spill of about 12,000 cubic feet of natural gas, BP

spokesperson Daren Beaudou said. There has been no impact to production from this latest leak at Prudhoe Bay, the largest oil field in the U.S., BP said. Pipeline corrosion was also behind an oil transit line leak that resulted in a March spill of an estimated record 200,000 gallons of crude oil. BP said it shut down the natural gas line immediately after discovering the leak, but did not publicly disclose the information because the amount of escaped natural gas came in below Alaska's reporting threshold.

Source: <http://go.reuters.co.uk/newsArticle.jhtml?type=businessNews&storyID=1183774&section=finance&src=rss/uk/businessNews>

5. *April 17, Reuters* — **U.S. Gulf workforce stretched as storm season looms.** With the next storm season looming, the U.S. energy industry is stretched thin as it struggles to rebuild Gulf of Mexico output from the ravages of hurricanes Katrina and Rita amid surging prices, officials said. Segments of the energy service and supply sector are having difficulty keeping enough workers on the job to move equipment and finish restoring platforms and pipelines in the region. The big thing is to keep crews working steadily, as many oil workers deal with rebuilding their own homes that were hit by hurricanes last autumn, said Ken Wells of the Offshore Marine Services Association (OMSA). Of the 55,000 people who work in the Gulf energy sector, most live along the coastlines of Texas, Louisiana, Mississippi, and Alabama. According to the U.S. Minerals Management Service's most recent figures, 23 percent of U.S. Gulf crude production and 14 percent of the gas output is still off-line. About five percent of the region's refining capacity is still down. In the first few months after the hurricanes, OMSA's member companies, which operate vessels that ferry supplies and people to and from offshore sites, lost entry-level deckhands to higher-paying reconstruction work onshore. But that has leveled off, Wells said.

Source: [http://news.yahoo.com/s/nm/20060417/us\\_nm/energy\\_gulfcoast\\_dc\\_1](http://news.yahoo.com/s/nm/20060417/us_nm/energy_gulfcoast_dc_1)

6. *April 17, Associated Press* — **Seabrook plant prepares for flu.** In addition to planning for terrorist attacks and equipment problems, officials at the Seabrook, NH, nuclear plant also are working on plans to keep the plant running safely in case employees are hit by a flu outbreak. Plant spokesperson Al Griffith says the main concern is having enough employees available to run the plant safely and efficiently.

Source: [http://www.wcax.com/Global/story.asp?S=4778294&nav=menu183\\_3\\_3\\_2](http://www.wcax.com/Global/story.asp?S=4778294&nav=menu183_3_3_2)

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

7. *April 17, KVIA (TX)* — **Chemical spill closes I-10 for several hours.** Texas Interstate 10 in El Paso was closed for several hours Monday, April 17, due to the rupturing of a bag of polyester beads carried by a big rig. Polyester beads in powder form are an inhalation hazard.

Source: <http://www.kvia.com/Global/story.asp?S=4780590&nav=AbC0>

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

8. *April 17, Associated Press* — **Boeing unveils restructuring of its operations in Kansas; company to lay off about 900 workers.** Citing defense budget cuts and delays, Boeing Co. announced Monday, April 17, it would restructure its Wichita, KS, operations and lay off about 900 workers or about 25 percent of its current work force at the plant. The Chicago-based company said its Wichita defense plant will focus on military 747 and wide-body aircraft modifications and upgrades. It also plans to continue its engineering center, focusing its engineering work on the B-52 Stratofortress and other defense and civil aviation related businesses. Boeing said it issued 60-day layoff notices to 360 workers on Tuesday, April 18. An additional 240 employees will lose their jobs by the end of July and 300 more jobs will be cut in mid-November, the company said. By the beginning of 2007, Boeing's Wichita defense plant will have about 2,700 workers, the company said.  
Source: [http://biz.yahoo.com/ap/060417/boeing\\_layoffs.html?v=8](http://biz.yahoo.com/ap/060417/boeing_layoffs.html?v=8)
9. *April 17, Defense News* — **U.S. Navy works to shrink submarine costs.** The U.S. Navy has begun an effort to redesign the forward sections of future SSN 774 Virginia-class submarines — one of several moves the service hopes can shrink the ships' \$2.4 billion price tag. Designers are trying to “dramatically simplify the bow,” said Rear Adm. William Hilarides, the Navy's program executive officer for submarines. At the heart of the effort is the proposed removal of the large spherical array of transducers that supports the BQQ-6 sonar system. The “ball” takes up most of the space inside the submarine's bow. A pattern of hydrophones on the hull would replace the sphere, Hilarides told reporters Monday, April 17, at the Washington, DC, Navy Yard. In place of the sphere, a payload integration module would be fitted to carry Tomahawk cruise missiles or other weapons. Twelve vertical launchers for Tomahawks are fitted in current versions of the class, placed just behind the sphere and its systems. Hilarides noted the redesign effort is “not a done deal” and has several issues to be resolved.  
Source: <http://www.defensenews.com/story.php?F=1692407&C=america>

[\[Return to top\]](#)

## **Banking and Finance Sector**

10. *April 18, Finextra* — **Debit card use outstrips cash for first time in UK.** Debit card spending in retail outlets exceeded cash spending for the first time ever in the UK last year, according to stats from payments association Apacs. The figures, which cover all online and offline retail transactions in 2005, show debit card spending at 37 percent of the total spent, against cash at 34 percent. Retail debit card use was up nine percent on 2004 figures, while cash retail spending fell four percent.  
Source: <http://finextra.com/fullstory.asp?id=15197>
11. *April 17, San Francisco Examiner* — **New laws yet to slow down phishing.** It's been six months since Governor Schwarzenegger signed the state's anti-phishing law, but it doesn't seem to be working. Oliver Friedrichs of Symantec Security Response reports he currently tracks 7.9 million phishing e-mails a day, an increase of 39 percent from 2005. The Anti-Phishing Act allows victims to sue for the amount of damages incurred or \$500,000, whichever is greater. The problem, according to Craig Cardon, a partner specializing in intellectual property and advertising with the law firm Sheppard, Mullin, Richter & Hampton LLP in San Francisco, is that phishers operate too far underground. “It's rare that you'll find the

person who sent you the phishing e-mail or they won't have the money to pay damages and if they do, they're set up offshore...The anti-phishing law is really symbolic," he said.

Source: [http://www.examiner.com/Business-a79916~New\\_laws\\_yet\\_to\\_slow\\_down\\_phishing\\_.html](http://www.examiner.com/Business-a79916~New_laws_yet_to_slow_down_phishing_.html)

12. *April 17, Computerworld* — **FBI: No credit card data breach in New Hampshire state server case.** An FBI investigation has concluded that no consumer credit or debit card information was stolen from a New Hampshire state computer server in February because a suspect Cain & Abel password recovery program found on the hardware had never been activated. In an announcement on Friday, April 14, New Hampshire Attorney General Kelly Ayotte said that the FBI probe determined that no data theft occurred because the program, which can be misused by hackers for malicious purposes, was never run. "As a result of this finding, the state has concluded that it is very unlikely that any credit card or debit card information was accessed by identity thieves," Ayotte said. The FBI, the U.S. Department of Justice, and New Hampshire officials began investigating the potential security breach after Cain & Abel was found on a state server during a routine security check two months ago. The New Hampshire Division of Motor Vehicles and the state Veterans Home used the server to transmit financial information, while the New Hampshire Liquor Commission used it as a backup for sales transactions. The inquiry led officials to place an unnamed Office of Information Technology employee on paid leave as part of the investigation.

Source: <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,110612,00.html>

13. *April 15, Websense Security Labs* — **Phishing Alert: Three Rivers Federal Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Three Rivers Federal Credit Union, which is based in Indiana. Users receive a spoofed e-mail message, which claims that their account will be suspended unless it is updated. This message provides a link to a phishing Website that prompts users to enter account information.

Source: <http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=466>

[[Return to top](#)]

## **Transportation and Border Security Sector**

14. *April 18, Department of Homeland Security* — **DHS completes international "e-Passport" live test.** Department of Homeland Security (DHS) Deputy Secretary Michael Jackson has announced important progress in the development of biometrically-enabled technologies to prevent the use of fraudulent or stolen international travel documents. DHS is testing e-Passports and e-Passport readers in anticipation of an upcoming deadline requiring all Visa Waiver travelers issued a passport after October 26, 2006, to present an e-Passport to enter the United States under the Visa Waiver Program (VWP). The use of the new e-Passports and deployment of e-Passport readers to U.S. ports of entry will help to ensure the authenticity of international travel documents and provide U.S. Customs and Border Protection officers with another invaluable tool for use in the border inspection process. The U.S. anticipates the deployment of e-Passport readers for processing VWP visitors by October 26, 2006. Recently, US-VISIT conducted a successful test of e Passports and e-Passport readers with Basic Access Control at San Francisco International Airport The test, which was conducted between January

15, 2006, and April 15, 2006, evaluated the operational impact of reading and verifying information embedded in the e-Passports on the border inspection process. This test was a collaborative effort between the United States, Australia, New Zealand and Singapore.  
Source: <http://www.dhs.gov/dhspublic/display?content=5541>

15. *April 18, Agence France-Presse* — **Vietnam Air and American Airlines begin passenger-sharing alliance.** Vietnam Airlines and American Airlines began a code-sharing agreement on Monday, April 17, an official of Vietnam's state-owned airline said. The agreement will allow the airlines to expand their reach by selling and marketing seats on each other's flights.  
Source: [http://www.usatoday.com/travel/flights/2006-04-18-aa-vietnam\\_x.htm](http://www.usatoday.com/travel/flights/2006-04-18-aa-vietnam_x.htm)
16. *April 17, Palm Beach Post (FL)* — **Port pursuing plan for huge South Florida cargo terminal.** Palm Beach County, FL, port officials have proposed building a large inland cargo terminal in South Bay, which could create sweeping changes in the flow of goods throughout South Florida, alleviate the amount of truck traffic on major highways and help revive this economically depressed farming region. The "inland port intermodal cargo industrial complex" would be built near the nexus of U.S. 27 and State Road 80, on the western edge of the county, on land primarily used for sugar cultivation. Cargo arriving through the port could be transported to the new terminal, stored there, broken up into smaller shipments if necessary, and redistributed. The new grid would reduce freight traffic on busy highways and rail lines that run near the coast of South Florida and transfer that traffic to lesser used inland roads and rail lines. It would connect to ports not only in Palm Beach but also Broward and Miami-Dade counties as well as the Gulf Coast. In addition, the new terminal would allow for greater growth of cargo operations at the Port of Palm Beach.  
Source: [http://www.palmbeachpost.com/localnews/content/local\\_news/eper/2006/04/17/sla\\_port\\_0417.html](http://www.palmbeachpost.com/localnews/content/local_news/eper/2006/04/17/sla_port_0417.html)
17. *April 17, KOMO TV (WA)* — **Mystery silence at Sea-Tac control tower prompts investigation.** For 25 minutes in the early hours of April 11, the control tower at Seattle-Tacoma International Airport (Sea-Tac) did not respond to airplane traffic. "There were two planes affected -- one trying to take off and one trying to come in," airport spokesperson Bob Parker said Monday, April 17. The unexplained silence, which started at 3:15 a.m. PDT, ended at 3:40 a.m. when a Port of Seattle staff member drove to the guard shack at the base of the control tower. Airport officials said that a Boeing 747-400 flown by Taiwanese carrier EVA was on its final approach to Sea-Tac when it radioed the control tower for permission to land. There was no response. Eventually, the airliner reached a dispatcher at the airport's departure control facility, who is not in the control tower, and made a plan to remain airborne until a controller could be reached. Meanwhile, a Delta Airlines jet attempting to back away from the airport's south satellite got no response when it sought clearance to leave. The matter is being investigated by the Federal Aviation Administration.  
Source: <http://www.komotv.com/stories/42986.htm>
18. *April 16, East Bay Business Times (CA)* — **California's two northern ports teaming up.** An unprecedented alliance between the ports of Sacramento and Oakland is expected to benefit both and drive economic expansion in West Sacramento. That's according to Omar Benjamin, director of commercial real estate for the Port of Oakland, and Mike Luken, the Port of

Sacramento's manager. "As the movement of goods becomes an increasingly important issue, we are attempting to create a one-stop shop for customers and manufacturers looking to move goods through Northern California," Benjamin said, noting that the volume of international cargo handled by U.S. ports will double between 2006 and 2020. "We see efficiencies, economies of scale and environmental benefits from this alliance," he said. Specifically, the Port of Oakland – grappling with increasing volumes of imported goods from Asia – would benefit from diverting cargo to Sacramento, he added. The Port of Oakland is the nation's fourth-busiest container port and Sacramento, as a "bulk" rather than container port, now handles about 800,000 tons of goods annually.

Source: <http://msnbc.msn.com/id/12349996/>

19. *April 14, Tampa Bay Business Journal* — **Federal port ID cards delayed, but Florida moves forward.** The federal identification cards mandated for all port personnel after the September 11, 2001, terrorist attacks have been delayed several times despite announcements of renewed efforts. Now, Florida is making a push to go ahead with its own version of the program in an attempt to make its 12 ports more secure. If it does that, there is concern that, when and if a federal program does come together, workers around Florida may have to pay or go through the process twice. Two months ago, after no notice from the Transportation Security Administration (TSA), Florida officials contacted TSA and informed it that it had an alternate solution. It planned to work with GE Security Systems in an attempt to move forward issuing a biometric credential modeled on the federal ID card.

Source: <http://tampabay.bizjournals.com/tampabay/stories/2006/04/17/story6.html>

[[Return to top](#)]

## **Postal and Shipping Sector**

Nothing to report.

[[Return to top](#)]

## **Agriculture Sector**

20. *April 18, American Farm* — **Mandatory registration to speed response to avian disease.**

Poultry diseases like exotic Newcastle disease and avian influenza know no state lines or neighbors' fences. Preventing and being able to contain diseases like these are so important that the Maryland General Assembly passed legislation in 2005 requiring domestic poultry and exotic bird premises to be registered with the state. To this end, the Maryland Department of Agriculture (MDA) Tuesday, April 18, announced the new Domestic Poultry and Exotic Bird premises registration program. Registration information will be filed with the Secretary of Agriculture. The registration process will take place in three phases. First, backyard flocks, including fair and show birds, will be registered. Then, certain categories of exotic and pet birds will be registered, followed by the final phase, registration of commercial flocks.

Source: <http://www.americanfarm.com/TopStory4.18.06i.html>

21. *April 17, Associated Press* — **Animal identification system won't require birth date.** A livestock tracking system planned by the government will not include the age of animals,

despite the key role age has played in mad cow disease investigations. U.S. Department of Agriculture (USDA) officials say they don't want to overburden ranchers and can track most birth dates. The USDA promised to create the system after the nation's first case of mad cow disease two years ago and has already spent \$84 million on it.

Source: <http://abcnews.go.com/Politics/wireStory?id=1852408>

[\[Return to top\]](#)

## **Food Sector**

Nothing to report.

[\[Return to top\]](#)

## **Water Sector**

Nothing to report.

[\[Return to top\]](#)

## **Public Health Sector**

### **22. *April 18, Agence France–Presse* — Bird flu experts in Vietnam to aid long–term control.**

More than 20 international animal and human health experts are visiting Vietnam this week to help the country move from its bird flu emergency response to long–term control, a United Nations (UN) official said. "The thing Vietnam is pushing for is restructuring its poultry sector, moving live bird markets out of cities, building new facilities and slaughter houses," Fabio Friscia of the UN Food and Agriculture Organization said on Tuesday, April 18. "They also want to upgrade their veterinary and human health services." Experts from the World Bank, World Health Organization, UN Development Program, FAO, Asian Development Bank and European Union and New Zealand aid agencies were taking part in the two–week mission that started Monday.

Source: [http://news.yahoo.com/s/afp/20060418/hl\\_afp/healthfluvietnam\\_un\\_060418104038](http://news.yahoo.com/s/afp/20060418/hl_afp/healthfluvietnam_un_060418104038)

### **23. *April 18, Reuters* — Sudan finds one man, five chickens with bird flu virus.** Sudan has found one man and five chickens infected with the bird flu virus, an official from the Health Ministry told Reuters on Tuesday, April 18. Head of the epidemics department, Magdi Salih, said tests carried out by Sudanese authorities on the man and the chickens had proved positive for bird flu, but he did not say if the virus was the H5N1 strain. The infected chickens were found at two farms in Sudan's Khartoum and Jazeera provinces and he added that the infected man was the owner of one of the farms. Samples would be sent abroad for further tests, he said. The H5N1 strain of bird flu has been confirmed in neighboring Egypt, which has reported four human deaths from the virus.

Source: <http://www.alertnet.org/thenews/newsdesk/L18711774.htm>

### **24. *April 18, Agence France–Presse* — China confirms new human case of bird flu.** China has confirmed its 17th human case of bird flu, reporting an urban case that suggested the virus might be gradually spreading to the cities. The patient is a 21–year–old man who was

employed as a migrant worker in the large industrial central city of Wuhan, the ministry said Tuesday, April 18. He started showing symptoms on April 1 and was diagnosed with the potentially lethal H5N1 strain on Monday, April 17. He is currently hospitalized in Wuhan. Source: [http://news.yahoo.com/s/afp/20060418/hl\\_afp/healthchinaflu\\_0\\_60418134301](http://news.yahoo.com/s/afp/20060418/hl_afp/healthchinaflu_0_60418134301)

25. *April 17, Johns Hopkins Bloomberg School of Public Health* — **Nearly half of public health employees unlikely to work during pandemic.** Over 40 percent of public health employees surveyed said they are unlikely to report to work during an influenza pandemic, according to researchers at the Johns Hopkins Bloomberg School of Public Health and Ben-Gurion University of the Negev in Israel. Local public health workers would play a vital role in responding to a pandemic, from monitoring the spread of illness, to organizing the distribution of medications, to communicating critical health information to the public. The survey, conducted in Maryland by the Bloomberg School's Center for Public Health Preparedness, also found that 66 percent of public health workers felt they would put themselves at risk of infection if they were to report to work during a pandemic. For the study, researchers surveyed 308 public health workers from three Maryland counties. The counties, Carroll, Dorchester and Harford, were selected because their population sizes were comparable to those covered by 96 percent of the nation's public health departments serving communities of 500,000 people or fewer. In the survey, clinical staff members, such as physicians and nurses, were more likely to say they would report for work. Technical or support staff were the least likely to say they would report to work.

Source: [http://www.jhsph.edu/publichealthnews/press\\_releases/2006/barnett\\_workforce.html](http://www.jhsph.edu/publichealthnews/press_releases/2006/barnett_workforce.html)

26. *April 17, Associated Press* — **Experts say elderly need better flu shot.** Seasonal flu kills elderly Americans in droves every winter because the vaccine simply doesn't work as well inside aging bodies as young ones. The National Institutes of Health (NIH) wants to strengthen flu shots destined for the elderly, part of a push to get the nation to start treating influenza's yearly attack as seriously as the threat of some super-flu striking in the future. "My great frustration (is) in trying to shake the cage and say, 'We have not, by any means, optimized how we approach seasonal flu,'" Anthony Fauci, the NIH's infectious disease chief, told The Associated Press. Topping his do-better list: testing whether higher vaccine doses or adding immune-boosting compounds to the shots — some of the same compounds already being studied to fight bird flu — would improve the elderly's protection against regular winter influenza. And NIH recently began recruiting 150 U.S. volunteers to study just which parts of the immune system change as we age to make flu a more serious threat, basic biological underpinnings that remain a mystery despite influenza's unrelenting yearly toll.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/04/17/AR2006041700892.html>

27. *April 17, Associated Press* — **Mumps cases spread in Nebraska, eight other states.** Nebraska, which is part of a nine-state mumps epidemic, is now reporting 110 cases of the disease in 22 counties, health officials said Monday, April 17. Thirty-two of those cases are confirmed. The mumps epidemic is the nation's first in 20 years. Some 600 suspected cases have been reported in Iowa. There are also cases reported in Kansas, Illinois, Indiana, Michigan, Missouri, Wisconsin and Minnesota. Mumps is a viral infection of the salivary glands. Symptoms include fever, headache, muscle aches and swelling of the glands close to the jaw. It can cause serious complications, including meningitis, damage to the testicles and

deafness. No deaths have been reported from the current epidemic. A mumps vaccine was introduced in 1967.

Source: <http://abcnews.go.com/Health/wireStory?id=1852477>

[[Return to top](#)]

## **Government Sector**

Nothing to report.

[[Return to top](#)]

## **Emergency Services Sector**

**28. *April 17, U.S. Department of Defense* — Defense agency prepared for 2006 hurricane season support.** Following an unprecedented domestic disaster relief effort in 2005, Defense Logistics Agency (DLA) officials in Fort Belvoir, VA, say DLA is ready to provide support during the 2006 hurricane season, which begins June 1. A recently completed agency-wide review of DLA's response to domestic disasters in 2005 was an opportunity for the headquarters and field activities staff to assess agency support, evaluate actions necessary to improve that support and to be prepared for similar missions in 2006, officials said. To ensure effective relief support during the upcoming hurricane season, DLA co-hosted a domestic disaster response logistics working group meeting last week in Springfield, VA, along with several top-level Pentagon organizations. The working group participants included U.S. Northern Command, U.S. Transportation Command, the National Guard Bureau, Army Materiel Command and the Federal Emergency Management Agency. The meeting focused on the synchronization of ongoing logistics preparation for domestic disasters.

Source: [http://www.defenselink.mil/news/Apr2006/20060417\\_4839.html](http://www.defenselink.mil/news/Apr2006/20060417_4839.html)

**29. *April 17, Fort Bend Herald (TX)* — Mock hurricane drill in Texas to focus on recovery efforts and debris management.** Hurricane season begins in June, and a drill to be conducted by the Fort Bend County, TX, Emergency Management Office will test the readiness of county and city governments. The exercise Wednesday, April 19, will involve Richmond, Rosenberg, Sugar Land, Stafford and Missouri City, in addition to Fort Bend County personnel. The drill is a continuation of 2005's "Hurricane Harley" drill, which focused on how county departments would react to an approaching storm in the Gulf Coast. This year's drill will focus recovery efforts and debris management just after a storm passes through Fort Bend County.

Source: [http://www.herald-coaster.com/articles/2006/04/17/news/news0\\_2.txt](http://www.herald-coaster.com/articles/2006/04/17/news/news0_2.txt)

**30. *April 17, Associated Press* — South Carolina researchers bring back Gulf Coast findings.** A group of University of South Carolina researchers canvassed New Orleans collecting fresh data — information on the human condition, environmental effects and policy response — that would lose its value if researchers waited too long to collect it. Among the findings presented Tuesday, April 18, at the CRISIS National Summit in Columbia, SC: The Army Corps of Engineers spent six days on an impracticable sandbagging approach to repair breached New Orleans levees. Civil engineering researcher Ahmed A. Kassem worked with graduate students to create a scale model of the 17th Street Canal, the site of the most serious breach of New

Orleans' levees. His conclusion: Using sandbags to patch the levees at the site of the breach was never practicable. It would have taken 50,000-pound sandbags to hold back the storm waters rushing into the city's neighborhoods. Kassem and a team of other researchers visited New Orleans to gather data and talk to officials about the levee system. They created what they say is a more effective model. It involves several rows of sandbags, with the sandbags getting heavier and the rows taller as they get closer to the levee.

CRISIS National Summit Website: <http://ced.sc.edu/crisis/>

Source: <http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/local/14363562.htm>

31. *April 17, New York Times* — **Alabama seeks to supplant Red Cross.** Frustrated with the performance of the American Red Cross, Alabama's governor has asked Department of Homeland Security Secretary Michael Chertoff for the federal aid necessary to let the state assume primary responsibility for operating its own emergency shelters in disasters. The move comes after months of criticism of the Red Cross, inspired by what even the organization's own leaders acknowledge was its inadequate response to Hurricane Katrina last year. Governor Bob Riley said that too often the Red Cross shelters did not have all the necessary services or equipment, like showers and cafeterias, which became a particular problem when evacuees ended up living in the shelters for weeks. To avoid that, Riley said he would like to establish a network of official state shelters at 30 state junior colleges that could accommodate a total of 25,000 evacuees.

Source: [http://www.nytimes.com/2006/04/18/us/nationalspecial/18alabama.html?\\_r=1&oref=slogin](http://www.nytimes.com/2006/04/18/us/nationalspecial/18alabama.html?_r=1&oref=slogin)

32. *April 17, Tennessean* — **Tornado blew through emergency plans' cracks, exposing gaps.** Hours-long traffic tie-ups and a few communication issues because of incompatible radio systems and downed phone lines were some of the glitches the Friday, April 7, tornado exposed in Sumner County, TN's, emergency planning. Authorities did a good job posting police to keep looters out of storm-struck neighborhoods, but a system of issuing orange pass cards to residents did not work, said Gallatin Mayor Don Wright. The identifying cards were supposed to help residents get to and from their homes in the protected neighborhoods, but many did not know where to get the passes or couldn't get there, Wright said. Next time, he said, he'd like to see the passes handed out to residents on-site. Wright is also contemplating a network of sirens for the city. If city power had gone out before tornado warnings for the city were issued, the town's lone siren would not have been effective in alerting residents, he said. All over the storm-struck region, cell phones played a key role as a back-up communication device. However, if cell towers are damaged or cell lines are jammed, this over-dependence on cell phones could be fatal, said Wright, who has become a fan of satellite phones.

Source: <http://www.tennessean.com/apps/pbcs.dll/article?AID=/20060417/NEWS02/604170340/1009/NEWS>

33. *April 17, Record Net (CA)* — **Dispatch dispute sets off alarms.** San Joaquin County, CA's, 911 medical dispatching system will split in two Monday, May 1, unless city and county officials resolve a dispute, feeding fears of miscommunication and chaos. Medical emergency calls received by the county Sheriff's Office, the California Highway Patrol, and the Escalon and Ripon police departments will be directed to American Medical Response's (AMR) operations center in Stanislaus County on May 1 — the day the county's exclusive ambulance contract with AMR goes into effect. All 911 calls from cellular phones also will be directed to

AMR. But emergency calls received by police departments in Stockton, Tracy, Lodi and Manteca instead will be routed through the Stockton Fire Department, which currently dispatches ambulances throughout most of the county. The result could be delays and confusion among fire department paramedics and AMR's ambulances, observers say. The Stockton Fire Department and AMR have yet to link their computerized communications systems together. The two agencies also will be working on different radio channels and frequencies — a problem when paramedics and first responders require updates from one another on medical situations, Stockton Fire Chief Ron Hittle said.

Source: <http://www.recordnet.com/apps/pbcs.dll/article?AID=/20060417/NEWS01/604170326/1001>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

34. *April 18, Security Focus* — **Linux kernel ptraced child auto reap local denial-of-service vulnerability.** Several local and remote vulnerabilities have been discovered in the Linux kernel that may lead to a denial-of-service or the execution of arbitrary code. Analysis: The kernel improperly auto reaps processes when they are being ptraced, leading to an invalid pointer. Further operations on this pointer result in a kernel crash. This issue allows local users to crash the kernel, denying service to legitimate users. For a complete list of vulnerable products: <http://www.securityfocus.com/bid/15625/info>  
Solution: Please see the referenced vendor advisories for further information on obtaining and applying the appropriate updates: <http://www.securityfocus.com/bid/15625/references>  
Linux kernel versions 2.6.15-rc3 and 2.6.14.3 have been released to address this issue.  
Source: <http://www.securityfocus.com/bid/15625/discuss>
35. *April 18, Security Focus* — **Linux kernel ICMP\_push\_reply remote denial-of-service vulnerability.** Linux kernel is prone to a remote denial-of-service vulnerability. Remote attackers can exploit this to leak kernel memory. Successful exploitation will result in a crash of the kernel, effectively denying service to legitimate users. For a complete list of vulnerable products: <http://www.securityfocus.com/bid/16044/info>  
Solution: Vendor upgrades are available. Please see the referenced vendor advisories for further information: <http://www.securityfocus.com/bid/16044/references>  
Source: <http://www.securityfocus.com/bid/16044/discuss>
36. *April 18, BBC News (UK)* — **Firms slow to fix security flaws.** Hackers are getting a helping hand from firms taking too long to fix software vulnerabilities, research shows. A study carried out for security firm McAfee found that 19 percent of companies take more than a week to apply software patches to close vulnerabilities. A further 27 percent said it took two days to apply fixes for software loopholes. Across Europe, the French took the longest to apply patches. It took 27 percent of French firms a week to fix loopholes and a further 39 percent had them applied in 48 hours.  
Source: <http://news.bbc.co.uk/2/hi/technology/4907588.stm>
37. *April 17, National Coordination Office for Networking and Information Technology Research*

*and Development* — **National Science and Technology Council releases Federal Plan for Cyber Security and Information Assurance Research and Development report.** The National Science and Technology Council, a Cabinet-level council that coordinates science and technology policies across the federal government, released the Federal Plan for Cyber Security and Information Assurance Research and Development Monday, April 17. This report sets out a framework for multi-agency coordination of federal research and development (R&D) investments in technologies that can better secure the interconnected computing systems, networks, and information that together make up the U.S. information technology infrastructure. The Federal Plan for Cyber Security and Information Assurance outlines strategic objectives for coordinated federal R&D in cyber security and information assurance (CSIA). The Plan presents a broad range of CSIA R&D technical topics and identifies those topics that are multi-agency technical and funding priorities. The plan's findings and recommendations address R&D priority-setting, coordination, fundamental R&D, emerging technologies, road-mapping, and metrics. Electronic pre-print release of the Federal Plan for Cyber Security and Information Assurance Research and Development: [http://www.nitrd.gov/pubs/csia/FederalPlan\\_CSIA\\_RnD.pdf](http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf)  
Source: [http://www.nitrd.gov/pubs/csia/FederalPlan\\_CSIA\\_RnD\\_Press.pdf](http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD_Press.pdf)

38. *April 17, eWeek* — **New attack is aimed at computers infected with Bagle virus.** A new attack aimed at computers infected with the Bagle virus threatens to generate scads of spam e-mail campaigns, and anti-malware experts concede that the threat remains a major headache. Researchers at anti-virus specialist F-Secure, based in Helsinki, Finland, described the attack, dubbed "SpamTool.Win32.Bagle.g," and said it involves a new set of URLs being sent to machines infected with Bagle. The variant is meant to use the computers to launch waves of spam messages and involves a download link that provides a new, uniquely repacked version of the attempted spam execution every 50 seconds or so, according to F-Secure. The new attack involved at least five different URLs used to distribute the new SpamTool execution, at least four of which have already been shut down, F-Secure said.

Source: <http://www.eweek.com/article2/0.1895.1950098.00.asp>

39. *April 17, Federal Computer Week* — **Center unveils online XML toolkit.** Researchers at the Center for Technology in Government at the State University of New York at Albany released its first version of an online toolkit Monday, April 17, designed to help government agencies use Extensible Markup Language (XML) for managing Websites. The toolkit offers a library of resources needed to manage a Website with XML.

The XML Toolkit: <http://www.thexmltoolkit.org/>

Source: <http://www.fcw.com/article94094-04-17-06-Web>

40. *April 17, Government Computer News* — **University of Pennsylvania students research wiretap vulnerabilities.** A team of graduate students from the University of Pennsylvania working with a National Science Foundation grant set out to determine just how trustworthy the most common types of telephone wiretaps used by police and intelligence agencies are, said Professor Matt Blaze. The results of these taps are accepted uncritically by courts, Blaze said at the 2006 International Conference on Network Security being held in Reston, VA. "It turns out, it can fail in all sorts of unexpected ways," he said. The techniques exploit vulnerabilities in the single signaling and audio channel used in analog telephone systems. Blaze said the project was an attempt to establish some baselines for network security by assessing how easy it is to

conduct reliable eavesdropping on the century-old protocols used in analog voice phone systems.

Source: [http://www.gcn.com/online/vol1\\_no1/40428-1.html](http://www.gcn.com/online/vol1_no1/40428-1.html)

## Internet Alert Dashboard

### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of an active exploitation of a cross site scripting vulnerability in the eBay website. Successful exploitation may allow an attacker to take various actions, including the following:

Obtain sensitive data from stored cookies  
Redirect auction viewers to phishing sites where further disclosure of login credentials or personal information can occur  
Create auctions that use script to place login areas on the eBay website, where credentials may be sent to a remote server with malicious intent

For more information please review the following advisory and vulnerability notes:

**CA-2000-02** – Malicious HTML Tags Embedded in Client Web Requests.

<http://www.cert.org/advisories/CA-2000-02.html>

**VU#808921** – eBay contains a cross-site scripting vulnerability.

<http://www.kb.cert.org/vuls/id/808921>

US-CERT recommends the following:

Securing Your Web Browser

[http://www.us-cert.gov/reading\\_room/securing\\_browser/#how\\_to\\_secure](http://www.us-cert.gov/reading_room/securing_browser/#how_to_secure)

Malicious Web Scripts FAQ

[http://www.cert.org/tech\\_tips/malicious\\_code\\_FAQ.html#steps](http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps)

eBay Spoof Email Tutorial

[http://pages.ebay.com/education/spooftutorial/spoof\\_3.html](http://pages.ebay.com/education/spooftutorial/spoof_3.html)

US-CERT Cyber Security Tip ST04-014.

<http://www.us-cert.gov/cas/tips/ST04-014.html>

Cyber Security Tip ST05-010. <http://www.us-cert.gov/cas/tips/ST05-010.html>

Add "ebay.com" to the Restricted Sites zone in Internet Explorer.

## Phishing Scams

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

## Current Port Attacks

<b>Top 10 Target Ports</b>	1026 (win-rpc), 6881 (bittorrent), 445 (microsoft-ds), 25 (smtp), 6348 (---), 32459 (---), 41170 (---), 1445 (proxima-lm), 32768 (HackersParadise), 135 (epmap) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## Commercial Facilities/Real Estate, Monument & Icons Sector

41. *April 18, Associated Press* — **Colorado man ticketed for changing red lights to green.** A Longmont man has been ticketed \$50 for suspicion of interfering with a traffic signal. Jason Niccum told Colorado's Longmont Times-Call that he bought a device that let him change traffic lights from red to green, called an Opticon, on eBay for \$100. He told the newspaper the device "paid for itself" in the two years he had it, helping him cut his time driving to work. Niccum was cited on March 29 after police said they caught him using the strobe-like device to change traffic signals. City traffic engineer Joe Olson said traffic engineers plan to update the city's system this year to block unauthorized light-changing signals. The Opticon devices, which are becoming more commonplace, are marketed through many different avenues. Dealers are instructed to sell only to "authorized users" such as volunteer first responders, doctors and security personnel, but it is easy for anyone to buy the devices online.  
Source: <http://www.wjactv.com/automotive/8768516/detail.html>

42. *April 18, Lenawee Connection (MI)* — **School security cameras on hold.** Security cameras for Adrian High School in Lenawee, MI, and two middle schools were put on pause Monday, April 17, as Adrian Public School (APS) trustees debated the cost of the new system and voted to review it again in two weeks. The proposed system is to digitally record activity in the most critical areas of Adrian's two middle schools, and nearly all areas of the high school — except for inside locker rooms and bathrooms. The system would help officials review such incidents as the start of an altercation, vandalism to the exterior of a building and, in cases such as a recent fire in a bathroom, who had entered or left the room. However, APS trustees Bob Stephan and Pat Cassidy expressed concern over the \$69,962 price. Trustees Jon Baucher and Ron Rowley both defended a camera system. Baucher noted that at a recent countywide

weekend assessment of youth assets, the top concern expressed by students was security. Rowley said that the system actually is a very inexpensive way of handling security, compared with having security officers present, and also will serve as a deterrent.

Source: <http://www.lenconnect.com/articles/2006/04/18/news/news06.txt>

- 43. April 18, Daily Times–Call (CO) — Gang–related graffiti continues to increase.** An explosion in gang–related graffiti in Longmont, CO, is forcing the city to reconsider how it responds to both taggers and their victims. Police point to apparently escalating gang involvement among the city’s youth as another prime reason for the increase in complaints. Graffiti, particularly the simple tags seen around Longmont, is considered a “billboard” or “newspaper” for gangs, serving as a way to mark territory and express their strength. The situation has gotten so bad that city manager Gordon Pedrow has ordered that some city vehicles be stocked with spray paint so workers who see graffiti on city property can immediately cover it up without having to call someone to do the work. Under city law, anyone with graffiti on their property is required to remove it within 10 days, even though that means the crime’s victim is held responsible for something a vandal did. That city law, created in 2000 and first enforced in 2002, has angered many property owners.

Source: <http://www.longmontfyi.com/Local–Story.asp?id=7251>

- 44. April 18, Associated Press — NYPD installs security cameras.** The New York Police Department has started installing the first of 500 security cameras in the city's streets and buildings as part of a plan modeled on London's video surveillance system. Police in New York have launched one of the country's most ambitious security schemes in an attempt to combat street crime and terrorism. Three police cameras, equipped with zoom lenses, have been installed on lamp posts, about 30 feet above the sidewalk, as part of a high–tech surveillance program. Hundreds of additional cameras could follow if the city receives the \$81.5 million in federal grants it has requested to safeguard Lower Manhattan and parts of midtown. The New York Police Department, which considers itself at the forefront of counter terrorism since the September 11 2001 attacks say revelations that al Qaeda once cased the New York Stock Exchange and other financial institutions, shows terrorists are focused on Lower Manhattan. Law enforcement and transportation agencies already have about 1,000 cameras in the subways, with 2,100 scheduled to be in place by 2008.

Source: [http://www.tampabays10.com/thismorning/thismorning\\_article.a.spx?storyid=28967](http://www.tampabays10.com/thismorning/thismorning_article.a.spx?storyid=28967)

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.